What Is A DDoS Attack?

- How Does a DDoS Attack Work?
- The Impact of DDoS Attacks
- The Impact of DDoS on Different Sectors
- The Social Ramifications of DDoS Attacks
- Radware's Data and Statistics on DDoS
- How to Identify a DDoS Attack
- The Main Types of DDoS Attacks
- How To Prevent DDoS Attacks
- How to Mitigate DDoS Attacks
- Legal and Ethical Considerations: Is DDoS a Crime?
- Future Trends and Predictions for DDoS Attacks

What is a DDoS Attack? | A Radware Minute

A DDoS attack, meaning a "Distributed Denial-of-Service (DDoS) attack", is an attack that occurs when multiple machines are operating together to attack one target to disrupt the normal traffic of a targeted server, service, or network, by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS allows for exponentially more requests to be sent to the target, therefore increasing the attack power. It also increases the difficulty of attribution, as the true source of the attack is harder to identify.

DDoS attacks can be devasting to an online business or any type of organization, which is why understanding how they work and how to mitigate them quickly is critical.

Common Motives Behind a DDoS Attack

Distributed Denial-of-Service (DDoS) attacks aren't launched in a vacuum. Perpetrators are driven by a range of motivations, transforming this tactic from a nuisance to a strategic tool. Understanding these motives is crucial for effective defense.

Ideological and Social Causes: Hacktivists, activists, and individuals with strong convictions may launch DDoS attacks to disrupt operations, raise awareness, or silence opposing voices. This can target government agencies, corporations, or organizations perceived as violating ethical principles or societal norms.

Financial Gain: DDoS attacks can be wielded as an extortion tool. Attackers may cripple an organization's online services and demand a ransom in exchange for restoring normalcy. This tactic often preys on businesses heavily reliant on online operations, forcing them into difficult choices.

Purely Destructive Acts: In some cases, DDoS attacks might be motivated by a desire for chaos or disruption. Perpetrators may find amusement in exploiting vulnerabilities and causing havoc, regardless of the specific target or desired outcome.

Malicious Competition: In the realm of business, DDoS attacks can be used by competitors to disrupt a rival's online presence and gain an unfair advantage. By overwhelming a competitor's servers, they aim to hinder their ability to serve customers and potentially damage their reputation.

Personal Grudges and Vendetta: DDoS attacks can be fueled by personal vendettas or disgruntled individuals seeking revenge against an organization or individual. This can manifest in attempts to disrupt online operations, damage reputation, or simply cause inconvenience.

By recognizing the diverse motivations behind DDoS attacks, organizations and individuals can develop more comprehensive and nuanced defense strategies. This may involve strengthening security protocols, implementing proactive mitigation measures, and staying informed about emerging threats and attack trends.

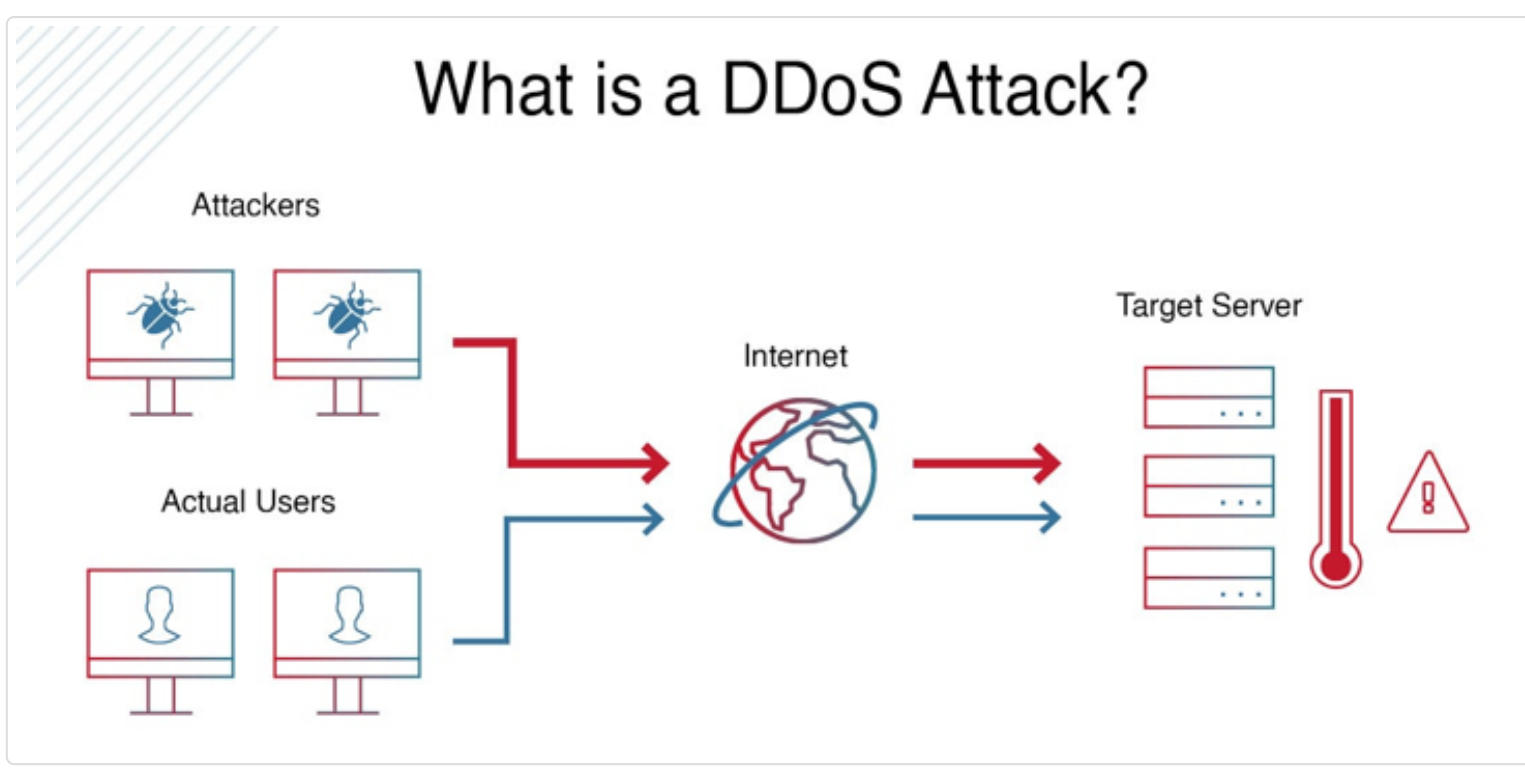

Figure 1: Basic Overview of a DDoS Attack

How Does a DDoS Attack Work?

Distributed Denial-of-Service (DDoS) attacks pose a significant threat to online operations, disrupting critical infrastructure and causing substantial financial losses. Understanding the intricate workings of these attacks is paramount for organizations and individuals alike to safeguard their online presence.

A Coordinated Deluge: Unlike traditional denial-of-service attacks originating from a single source, DDoS attacks unleash a coordinated and highly concentrated bombardment. Perpetrators wield a distributed network of compromised devices, known as a botnet. This "army" can encompass millions of unsuspecting personal computers, smartphones, and even Internet-of-Things (IoT) gadgets, unwittingly becoming tools in the malicious campaign.

Democratization of Disruption: The accessibility of botnets has emerged as a concerning trend. Malicious actors can now rent out these botnets through "attack-for-hire" services. This effectively lowers the technical barrier to entry for potential attackers, widening the pool and amplifying the potential impact of DDoS attacks. This necessitates heightened vigilance and the implementation of robust security measures to combat this evolving threat landscape.

Involuntary Participants: It is crucial to recognize that the **compromised devices within a botnet are involuntary participants**. They are not actively involved in the attack but rather unwitting victims, manipulated by the attacker to orchestrate the digital assault.

Exploiting Vulnerabilities: Attackers employ various tactics to commandeer these devices, including malware deployment or exploiting unpatched software vulnerabilities. Once compromised, these devices become mere puppets under the attacker's control, their resources and capabilities channeled towards a singular, malicious objective.

Shifting Targets: While traditional DDoS attacks may have focused on individual servers, they now often target the underlying network infrastructure. Attackers strategically target crucial components like routers and switches, aiming to saturate the network's bandwidth capacity. This effectively disrupts connectivity and hinders access to the targeted resources, causing significant downtime and potential financial losses.

By delving into the intricate mechanics of DDoS attacks and recognizing their evolving nature, organizations and individuals can equip themselves with the necessary knowledge to mitigate risks and bolster their online resilience.

The Impact of DDoS Attacks

Distributed Denial of Service (DDoS) attacks are a significant threat in the digital world. They aim to make online services unavailable by overwhelming them with traffic from multiple sources. **The impacts of these attacks are multifaceted, extending beyond immediate technical repercussions to broader economic and social ramifications**.

Technical Repercussions
At a technical level, DDoS attacks can cause severe disruptions to online services. They can lead to the unavailability of critical services, loss of productivity, and extensive remediation costs. The scale of these attacks has been rising tremendously with the advancement of the Internet of Things (IoT), making them a significant concern for cybersecurity.

DDoS attacks can create downtime, which can lead to **revenue loss and erode consumer trust**. They can also distract IT teams, giving hackers the chance to exploit other vulnerabilities, steal data, or infect a network with various forms of malware.

Economic Ramifications
The economic impact of DDoS attacks can be substantial. They **can cost an organization millions of dollars in terms of remediation costs**, lost revenue, lost productivity, loss of market share, and damage to brand reputation. Downtime can be extremely costly, depending on the type of business and the size of the organization.

Moreover, DDoS attacks can have indirect economic effects. For instance, they can lead to increased cybersecurity spending and higher insurance premiums. They can also result in regulatory fines if the attacks lead to data breaches or non-compliance with data protection regulations.

Social Impacts
The social impacts of DDoS attacks can be far-reaching. They **can erode trust in online services, leading to changes in user behavior**. For instance, users may become more hesitant to engage in online activities, such as online shopping or using online banking services, out of fear of potential DDoS attacks.

Furthermore, DDoS attacks can have societal impacts when they target critical infrastructure, such as power grids, healthcare systems, or public transportation systems. Such attacks can disrupt essential services, causing widespread inconvenience and even posing risks to public safety.

These case studies highlight the potential scale and impact of DDoS attacks, demonstrating the importance of effective mitigation strategies and the need for ongoing vigilance in the face of evolving threats.

Notable DDoS Attacks

The following case studies highlight the potential scale and impact of DDoS attacks, demonstrating the importance of effective mitigation strategies and the need for ongoing vigilance in the face of evolving threats.

Attack on LCK Spring 2024 (February 2024): Recent matches in the LCK Spring 2024 season faced disruptions caused by persistent ping issues attributed to DDoS attacks. These disruptions led to prolonged technical pauses, impacting players and fans, both online and on-site.

Attack on AWS (February 2020): Amazon Web Services (AWS) reported mitigating a massive DDoS attack that saw incoming traffic at a rate of 2.3 terabits per second (Tbps). The attackers responsible used hijacked Connection-less Lightweight Directory Access Protocol (CLDAP) web servers. AWS did not disclose which customer was targeted by the attack.

Attack on Google (September 2017): This attack is considered the largest DDoS attack to date, reaching a size of 2.54 Tbps. The attackers sent spoofed packets to 180,000 web servers, which in turn sent responses to Google. This was not an isolated incident as the attackers had directed multiple DDoS attacks at Google's infrastructure over the previous six months.

Attack on Occupy Central, Hong Kong (2014): This attack targeted the Occupy Central movement in Hong Kong. The movement's websites were hit with a massive DDoS attack, disrupting their online presence and communication.

Attack on Overwatch 2 (February 2024): The popular online multiplayer game Overwatch 2 was hit with a major DDoS attack. The attack caused major issues for players, disrupting gameplay and causing widespread frustration.

Attack on GitHub (February 2018): This attack reached 1.3 Tbps, sending packets at a rate of 126.9 million per second. The GitHub attack was a memcached DDoS attack, so there were no botnets involved. Instead, the attackers leveraged the amplification effect of a popular database caching system known as memcached. By flooding memcached servers with spoofed requests, the attackers were able to amplify their attack by a magnitude of about 50,000 times.

Attack on Dyn (October 2016): This massive DDoS attack was directed at Dyn, a major DNS provider. The attack created disruption for many major sites, including Airbnb, Netflix, PayPal, Visa, Amazon, The New York Times, Reddit, and GitHub. This was done using malware called Mirai, which creates a botnet out of compromised Internet of Things (IoT) devices such as cameras, smart TVs, radios, printers, and even baby monitors.

The Economic and Social Impact of DDoS Attacks

Direct Costs of DDoS Attacks

DDoS attacks can cause severe disruptions and financial losses for targeted organizations. The direct costs associated with these attacks include:

Loss of Revenue: A DDoS attack can disrupt an organization's online services, preventing potential customers from completing transactions and leading to significant revenue losses. This is particularly damaging for e-commerce platforms and businesses heavily reliant on online services.

Potential Ransom Payments: Some DDoS attacks are accompanied by ransom demands, adding to the financial burden on the targeted organization.

Mitigation Expenses: Implementing robust DDoS mitigation measures is essential for effectively thwarting attacks. Organizations may opt for hardware-based solutions, cloud-based protection, or hybrid approaches, each with varying costs dependent on the attack's scale and complexity.

The Impact of DDoS on Different Sectors

Let's look at the impact of DDoS attacks on various industries:

Finance and Technology

These sectors are prime targets for DDoS attacks due to their critical role in the global economy and the extensive use of online services.

Financial Implications

Revenue Loss: DDoS attacks can disrupt online banking, stock trading, and payment processing systems. The resulting downtime can lead to significant revenue losses.

Reputation Damage: Customers expect seamless online services from financial institutions. Any disruption can harm the institution's reputation and erode customer trust.

Regulatory Compliance: Financial organizations must comply with strict regulations regarding data security and availability. DDoS attacks can jeopardize compliance.

Technological Impact

Network Congestion: DDoS floods overwhelm network infrastructure, causing congestion and latency. This affects real-time transactions and communication.

Resource Exhaustion: Attackers target servers, firewalls, and load balancers, exhausting their resources and rendering them ineffective.

Mitigation Costs: Financial firms invest heavily in DDoS mitigation solutions to protect their systems.

Healthcare

Critical Services: Healthcare relies on digital systems for patient records, telemedicine, and medical equipment. DDoS attacks disrupt these services.

Public Health Impact: DDoS attacks on healthcare institutions can hinder pandemic response efforts, vaccination campaigns, and health information dissemination.

Supply Chain Disruption: Pharmaceutical companies, medical device manufacturers, and logistics providers face supply chain disruptions during attacks.

Patient Safety: Delayed access to medical records or emergency services due to DDoS attacks can endanger patient lives.

Education

Access to Resources: Libraries, research databases, and e-learning portals become inaccessible during attacks.

Online Learning Platforms: Educational institutions increasingly rely on online learning platforms. DDoS attacks disrupt classes, exams, and student collaboration.

Administrative Systems: DDoS attacks affect administrative functions such as student enrollment, payroll, and communication.

Student Experience: Downtime impacts student experience, especially during critical periods like exams or admissions.

Other Vulnerable Sectors

Government: Attacks on government websites can disrupt citizen services, tax filing, and public information dissemination.

E-Commerce: Retailers face revenue loss during peak shopping seasons due to DDoS attacks.

Gaming: Online gaming platforms experience latency, affecting user experience and in-game transactions.

Media and Entertainment: Streaming services, news websites, and social media platforms are vulnerable to DDoS attacks.

The Social Ramifications of DDoS Attacks

The social impacts of DDoS attacks can cause lasting damage to an enterprise, its customers, and its employees. These impacts include:

Impacts on Freedom of Expression: DDoS attacks can be used to target media outlets or political websites, potentially stifling freedom of expression and leading to censorship.

Potential for Escalation into Geopolitical Tensions: DDoS attacks can be used as tools in larger geopolitical conflicts, potentially escalating tensions between nations.

Erosion of Trust in Digital Services: DDoS attacks cast a shadow of doubt on an organization's ability to safeguard customer data and ensure reliable services. The erosion of trust among customers can cause long-term reputational damage, impacting brand loyalty and new customer acquisition.

Radware's Data and Statistics on DDoS

The economic and social impacts of DDoS attacks are far-reaching and multifaceted. They pose significant threats to businesses across sectors and can have profound societal implications. Therefore, it is crucial for organizations to understand these impacts and invest in robust defense strategies to mitigate the risks associated with DDoS attacks.

According to Radware's 2024 Global Threat Analysis Report, DDoS attacks are evolving, with hackers adapting their strategies to counteract growing mitigation techniques. In 2023, the number of DDoS attacks per customer **grew by 94%** compared to 2022, building on the previous year's growth of 99%. The number of attacks per customer has been trending at an average rate of 106 attacks per month or 3.48 attacks per day since Q1 2021. In Q1 of 2023, a typical Radware customer had to fend off an average of **49 attacks per day**.

The attack volume per customer **increased 48% in 2023** compared to 2022. In 2023, we observed 63% more attacks with traffic below 1Gbps, 177% more attacks peaking between 100Gbps and 250Gbps, and an increase of 150% in large attacks peaking above 500Gbps.

The Americas were targeted by almost half of all global DDoS attacks. The EMEA region, accounting for 39% of the DDoS attacks, had to mitigate 65% of the global DDoS attack volume. The APAC region accounted for almost 12% of global DDoS attacks.

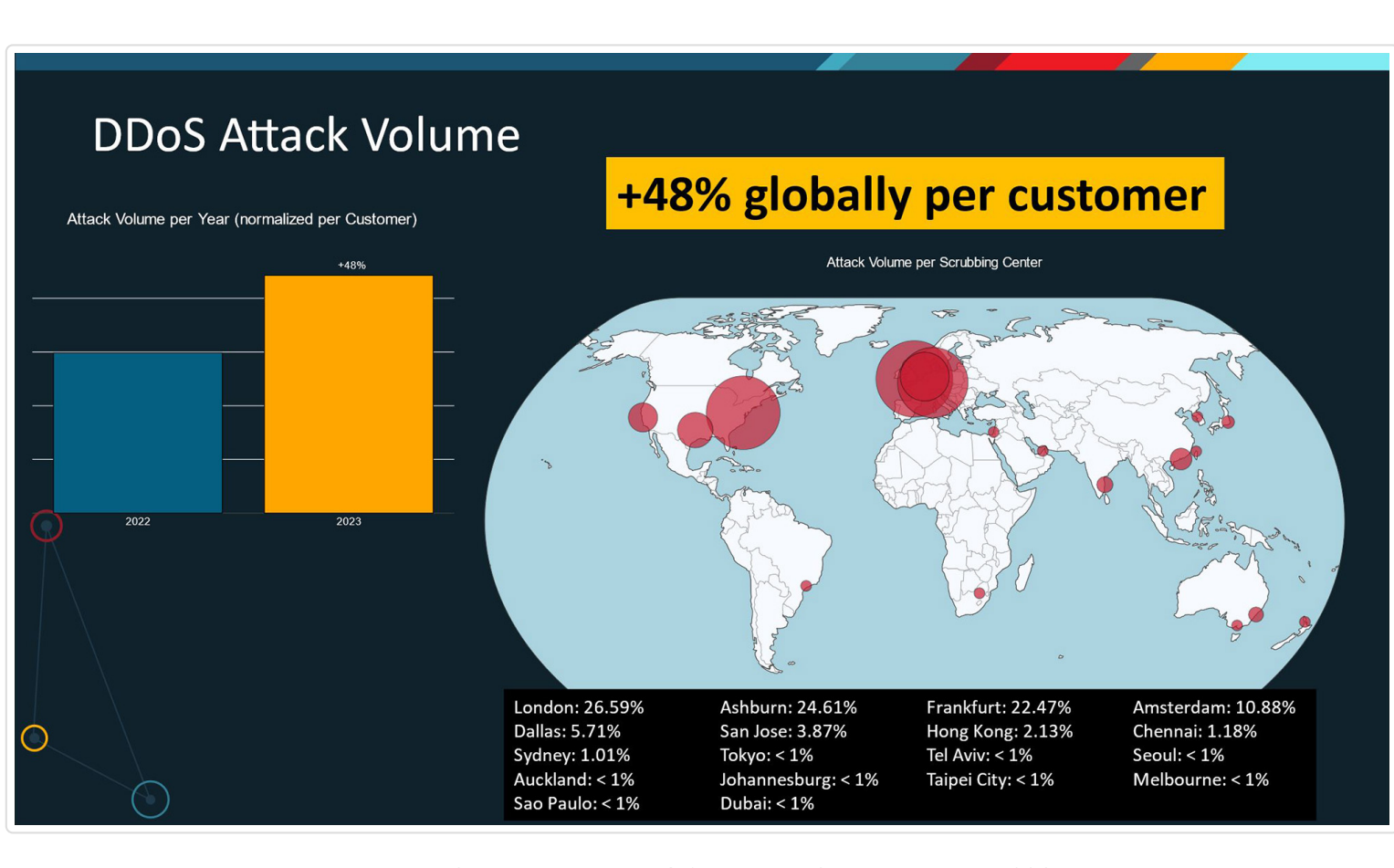

Figure 2: Increase in DDoS Attacks on Organizations in 2023

The Cost of DDoS Attacks

The cost of a DDoS attack can be calculated by considering both direct and indirect costs:

Direct Costs: These are costs associated with downtime/latency, loss of immediate revenue, and personnel costs associated with mitigating attacks. For instance, when a DDoS attack disrupts an organization's online services, potential customers cannot complete transactions, leading to significant revenue losses. Implementing robust DDoS mitigation measures is essential to thwarting attacks effectively. Organizations may opt for hardware-based solutions, cloud-based protection, or hybrid approaches, each with varying costs dependent on the attack's scale and complexity.

Indirect Costs: These would be customer churn, regulatory repercussions, and compromised data. For example, DDoS attacks cast a shadow of doubt on an organization's ability to safeguard customer data and ensure reliable services. The erosion of trust among customers can cause long-term reputational damage, impacting brand loyalty and new customer acquisition.

Costs Based on Radware Data

According to Radware's 2023 report Application Security in a Multi-Cloud World, **nearly one-third (31%) of organizations face DDoS attacks weekly**. Downtime due to a successful application DDoS attack costs organizations an average of **$6,130 per minute**. This means that even a short-lived DDoS attack can result in significant financial losses. **For instance, if an attack lasts for an hour, the cost could potentially escalate to over $367,800**.

The Importance of Investing in DDoS Prevention and Mitigation Strategies

Investing in effective DDoS mitigation technology enhances an organization's resiliency against nation-state adversaries and other malicious actors, making it a less attractive target. Rapidly mitigating DDoS attacks can save organizations time and money. As cybercriminals continue to evolve their tactics, implementing effective DDoS prevention strategies becomes imperative for safeguarding online operations, protecting critical services, and maintaining trust with users. While implementing a strong mitigation strategy against DDoS attacks can be time-consuming, having that strategy in place means you can have stronger peace of mind. More importantly, mitigation and catching early warning signs are ways to improve the strength of your organization's cybersecurity posture.

The cost of DDoS attacks can be substantial, and it's crucial for organizations to understand these costs and invest in robust defense strategies to mitigate the risks associated with DDoS attacks.

How to Identify a DDoS Attack

The best way to detect and identify a DDoS attack would be via network traffic monitoring and analysis. Network traffic can be monitored via a firewall or intrusion detection system. An administrator may even set up rules that create an alert upon the detection of an anomalous traffic load and identify the source of the traffic or drops network packets that meet certain criteria.

Symptoms of a DoS attack can resemble non-malicious availability issues, such as technical problems with a particular network or a system administrator performing maintenance. However, the following symptoms could indicate a DoS or DDoS attack:

- Unusually slow network performance
- Unavailability of a particular network service and/or website
- An inability to access any website
- An IP address makes an unusually large number of requests in a limited timespan
- Server responds with a 503-error due to a service outage
- Log analysis indicated a large spike in network traffic
- Odd traffic patterns such as spikes at odd hours of the day or patterns that appear to be unusual

The Main Types of DDoS Attacks

DDoS and network-layer attacks are as diverse as they are sophisticated. Due to the growing array of online marketplaces, it is now possible for attackers to execute DDoS attack with little to no knowledge of networks and cyberattacks. Attack tools and services are easy to access, making the pool of possible assaults larger than ever.

Here are four of the most common, and sophisticated, DDoS attacks currently targeting organizations:

Application Layer (Layer-7) DDoS Attacks

Application Layer DDoS attacks **specifically target the application layer of networked services**. Unlike traditional network-based attacks that flood network resources, these attacks exploit vulnerabilities in application protocols such as HTTP, HTTPS, SMTP, FTP, and VOIP. Their goal is to exhaust the resources of the targeted application, rendering it inaccessible or unresponsive to legitimate users.

Attack Vectors and Techniques

Application Layer DDoS attacks exhibit diverse characteristics:

HTTP Floods: Attackers flood web servers with a massive number of HTTP requests. These requests overload the server's processing capacity, leading to service disruption.

SMTP and Email Attacks: By bombarding email servers with excessive requests, attackers disrupt email communication and overload mail servers.

FTP Attacks: Attackers overwhelm File Transfer Protocol (FTP) servers, hindering file transfers and access.

HTTPS Attacks: Similar to HTTP floods, but with encrypted traffic. Attackers exploit SSL/TLS handshakes, consuming server resources during connection setup.

VOIP Attacks: Targeting Voice over IP (VOIP) services, these attacks flood SIP (Session Initiation Protocol) servers, causing call drops and service degradation.

Flavors of Application Layer Attacks

Application Layer DDoS attacks come in various flavors:

"Low and Slow" Attacks: These are more subtle. Attackers send requests at a slow pace, avoiding detection thresholds. For example:

> **Slowloris:** Opens multiple connections to a web server and sends partial HTTP requests, keeping connections open indefinitely.
>
> **R-U-Dead-Yet (RUDY):** Sends slow POST requests to exhaust server resources.

Flood Attacks: High-volume requests flood the application, saturating its resources. These can be HTTP floods, HTTPS floods, or other protocol-specific floods.

Impact and Challenges

Application Layer DDoS attacks exhibit diverse characteristics:

Resource Exhaustion: Application Layer DDoS attacks drain server memory, CPU, and bandwidth. This affects response times and overall performance.

Complex Attribution: Identifying the true

Mitigation Complexity: Unlike network-based attacks, application layer attacks require specialized defenses that inspect application-level traffic.

Service Disruption: Critical services like source of these attacks is challenging due to spoofed IP addresses and botnets.

web applications, email, and VOIP become unusable during attacks.

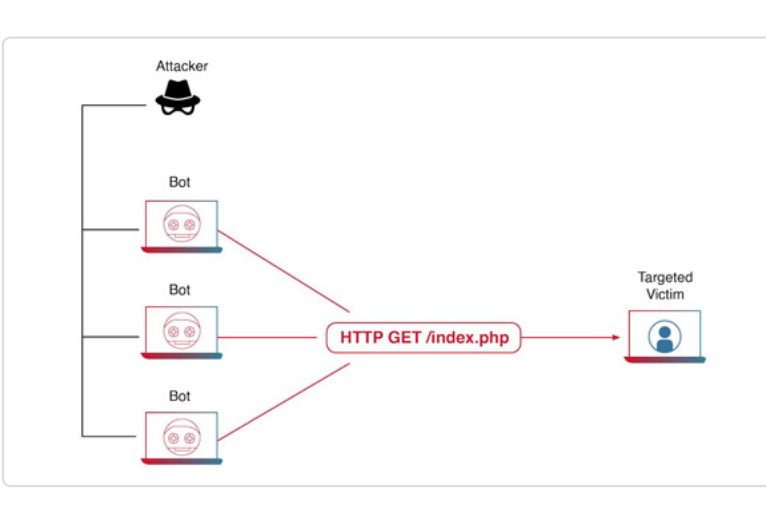

Figure 3: How a Layer-7 Application DDoS Attack

What is a Layer 7 DDoS Attack? | A Radware Minute

Volumetric or Volume-Based Attacks

Volumetric DDoS attacks have been a persistent threat in the cybersecurity landscape. **These attacks aim to overwhelm a network's bandwidth, causing disruptions in availability and accessibility**. The evolution of these attacks has been influenced by various geopolitical events and advancements in technology, including the advent of Reflection/Amplification attacks.

Volumetric DDoS attacks are characterized by several key features:

High Traffic Volume: These attacks generate an enormous amount of traffic, saturating the bandwidth of the targeted network.

Use of Botnets: Attackers often leverage botnets - networks of compromised devices - to generate the massive traffic volume required for these attacks.

IP Spoofing: Attackers often use IP spoofing to mask the source of the attack traffic, making it difficult to block and trace back.

Protocol Exploitation: Common network protocols such as NTP, DNS, and SSDP are exploited to amplify the attack traffic.

Reflection/Amplification Attacks: In these attacks, the attacker spoofs the victim's IP address and sends a request to a third-party server that will send a large response. This amplifies the amount of traffic directed at the victim, overwhelming their resources.

Impact and Challenges

Bandwidth Saturation: Volumetric DDoS attacks consume all available network bandwidth, affecting network speed and overall performance.

Mitigation Complexity: Unlike traditional network-based attacks, volumetric DDoS attacks require specialized defenses that can handle high volumes of traffic and distinguish between legitimate and malicious requests.

Service Disruption: Essential services such as web servers, databases, and cloud services become inaccessible during attacks.

Complex Attribution: Pinpointing the actual source of these attacks is challenging due to tactics like IP spoofing and the use of botnets.

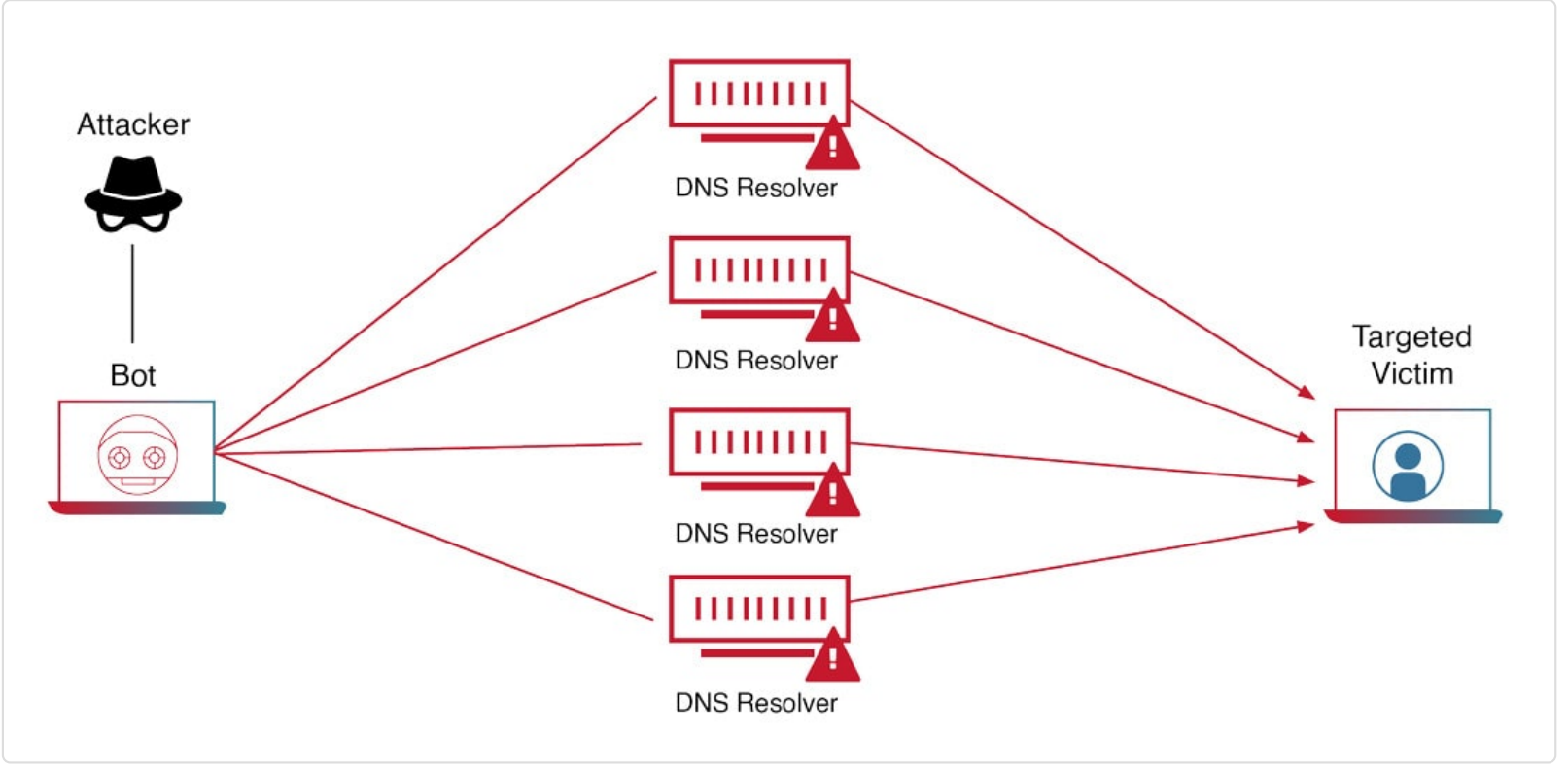

Figure 4: How a Volumetric DDoS Attack Works

Web DDoS Tsunami Attack

Web DDoS tsunami attacks represent a new breed of cyber threat that emerged during the heightened era of hacktivist activity triggered by Russia's invasion of Ukraine in February 2022. Initially, these attacks began as high-volume network-based Flood attacks. However, they swiftly evolved into more sophisticated multi-vector application-level assaults that pose significant challenges for detection and mitigation.

These attacks are characterized by several key features:

High Request Volume: Web DDoS Tsunami attacks generate an exceptionally high number of requests per second (RPS), overwhelming targeted servers and infrastructure.

Encryption: Attack traffic is often encrypted, making it difficult to discern malicious requests from legitimate ones.

Application-Level Attack Methods: These include HTTPS Get, Push, and Post request attacks with dynamic parameters behind proxies. Each request appears innocuous, making timely detection challenging.

Continuous Morphing: Web DDoS Tsunami attacks continuously evolve, altering their patterns and characteristics. This dynamic behavior prolongs the attack duration and exacerbates downtime.

Sophisticated Evasion Techniques:

> **Randomized Headers:** Attackers manipulate HTTP methods, headers, and cookies, making their requests appear legitimate.
>
> **IP Spoofing:** They spoof IP addresses, complicating attribution and filtering.
>
> **Impersonation of Third-Party Services:** Attackers mimic popular embedded third-party services, further camouflaging their intent.

Mitigation Challenges and Strategies

Mitigating Web DDoS Tsunami attacks poses unique challenges:

Resource Exhaustion: These attacks drain server memory, CPU, and bandwidth, affecting response times and overall performance.

Mitigation Complexity: Unlike network-based attacks, application layer attacks require specialized defenses that inspect application-level traffic.

Service Disruption: Critical services like web applications, email, and VOIP become unusable during attacks.

Complex Attribution: Identifying the true source of these attacks is challenging due to spoofed IP addresses and botnets.

To combat these attacks, **organizations need comprehensive application protection that combines real-time threat intelligence, behavioral analysis, and machine learning**. Such solutions can adapt to evolving attack techniques, detect anomalies, and mitigate sophisticated attacks while allowing legitimate traffic to flow unimpeded.

How to Prevent DDoS Attacks

To prevent DDoS attacks, there are several key capabilities organizations should consider to mitigate DDoS attacks, ensure service availability and minimize false positives. Leveraging behavioral-based technologies, understanding the pros and cons of different DDoS deployment options and having the ability to mitigate an array of DDoS attack vectors is essential to preventing DDoS attacks.

The following capabilities are critical to preventing DDoS attacks:

Scrubbing Capacity and Global Network
DDoS attacks are increasing in quantity, severity, complexity, and persistence. If faced with large volumetric or simultaneous assaults, cloud DDoS services should provide a robust, global security network that scales with several Tbps worth of mitigation capacity with dedicated scrubbing centers segregating clean traffic from DDoS attack traffic.

Multiple Deployment Options
Flexibility of deployment models is crucial so an organization can tailor its DDoS mitigation service to suit its needs, budget, network topology and threat profile. The appropriate deployment model—hybrid, on-demand or always-on cloud protection—will vary based on network topology, application hosting environments and sensitivity to delays and latency.

Behavioral-Based Protection
A DDoS mitigation solution that blocks attacks without impacting legitimate traffic is key. Solutions that leverage machine-learning and behavioral-based algorithms to understand what constitutes legitimate behavior and automatically blocks malicious attacks are critical. This increases protection accuracy and minimizes false positives.

Automation
With today's dynamic and automated DDoS attacks, organizations do not want to rely on manual protection. A service that does not require any customer intervention with a fully automated attack lifecycle—data collection, attack detection, traffic diversion and attack mitigation—ensures better quality protection.

Comprehensive Protection Against an Array of Attack Vectors
The threat landscape is consistently evolving. A DDoS mitigation solution that offers the widest protection, is not limited to just network-layer attack protection and includes protection against the aforementioned attack vectors is crucial.

How to Mitigate DDoS Attacks

There are several important steps and measures an organization can follow to mitigate a DDoS attack. This includes timely communication with both internal stakeholders and 3rd providers, attack analysis, activation of basic countermeasures (such as rate limiting) and more advanced DDoS mitigation protection, and analysis. Here are five steps to follow to mitigate a DDoS attack.

Step 1: Alert Key Stakeholders
Alert key stakeholders within the organization of the attack and steps that are being taken to mitigate it. Examples of key stakeholders include the CISO, security operations center (SoC), IT director, operations managers, business managers of affected services, etc. Keep the alert concise but informative.

Key information should include:

- What is occuring
- When the attack started
- What steps are being taken to mitigate the attack
- Impact to users and customers
- Which assets (applications, services, servers, etc.) are being impacted

Step 2: Notify Your Security Provider
You will also want to alert your security provider and initiate steps on their end to help mitigate the attack. Your security provider could be your internet service provider (ISP), web hosting provider or a dedicated security service. Each vendor type has different capabilities and scope of service. Your ISP might help you minimize the amount of malicious network traffic reaching your network, whereas your web hosting provider might help you minimize application impact and scale your service accordingly.

Likewise, security services will usually have dedicated tools for dealing with DDoS attacks. Even if you don't already have a predefined agreement for service, or are not subscribed to their DDoS protection offering, you should nonetheless reach out to them to see how they can assist.

Step 3: Activate Countermeasures
If you already have anti-DDoS countermeasures in place, activate them. Ideally, these countermeasures will initiate immediately when an attack is detected. However, in some cases, certain tools, such as out-of-path hardware devices or manually activated, on-demand mitigation services, might require the customer to initiate them manually.

One approach is to implement IP-based access Control lists (ACLs) to block all traffic coming from attack sources. This is accomplished at the network router level and can usually be accomplished by either your network team or your ISP. This is a useful approach if the attack is coming from a single source or a small number of attack sources. However, if the attack is coming from a large pool of IP address, this approach might not help.

If the target of the attack is an application- or a web-based service, you could limit the number of concurrent application connections. This approach is known as rate-limiting and is frequently the favored approach by web hosting providers and CDNs. Note that this approach is prone to high degrees of false positives because it cannot distinguish between malicious and legitimate user traffic. Dedicated DDoS protection tools will give you the widest coverage against DDoS attacks. DDoS protection measures can be deployed either as an appliance in your data center, as a cloud-based scrubbing service, or as a hybrid solution combining a hardware device and a cloud service.

Step 4: Monitor Attack Progression
Throughout the attack, monitor the progression of the attack to see how it develops. This should include:

- What type of DDoS attack is it? Is it a network-level flood or an application-layer attack?
- What are the attack characteristics? How large is the attack, both in terms of bits-per-second and of packets-per-second?
- How does the attack pattern look like? Is it a single sustained flood or is it a burst attack? Does it involve a single protocol, or does it involve multiple attack vectors?
- Is the attack coming from a single IP source or multiple sources? Can you identify them?
- Are the targets of the attack staying the same or are attackers changing their targets over time?

Tracking attack progression will also help you tune your defenses to stop it.

Step 5: Assess Defense Performance
Finally, as the attack develops and countermeasures are activated, assess their effectiveness. Your security vendor should provide a service level agreement document which commits their service obligations. Ensure they're meeting their SLAs and whether there is an impact to your operations. If they're not, or not able to stop the attack whatsoever, now is the time to assess whether you need to make an emergency change to your service.

Legal and Ethical Considerations: Is DDoS a Crime?

Legal Considerations
DDoS attacks are considered illegal in most countries and can lead to severe penalties.

Criminal Charges: DDoS attacks are illegal, and the attacker may face criminal charges. For instance, under the Computer Misuse Act 1990 in the UK, individuals involved in DDoS attacks face up to 10 years in prison. In the United States, individuals participating in DDoS attacks risk being charged with legal offenses at the federal level, both criminally and civilly.

Liability: If a DDoS attack causes harm to an individual or a business, the attacker can be held liable for the damages.

Violation of Terms of Service: DDoS attacks violate the terms of service of most internet service providers and websites.

Ethical Considerations
While DDoS attacks are generally viewed as malicious activities, some argue that they can serve a noble purpose by taking down harmful websites. However, this perspective is fraught with moral dilemmas and potential legal battles.

Potential for Abuse: Despite these arguments, DDoS attacks have the potential to be abused and can cause significant harm. They can disrupt services, cause financial loss, and infringe on people's rights to access information. Therefore, even if they are used with good intentions, DDoS attacks can have negative consequences.

Civil Disobedience: Some proponents of DDoS attacks argue that they can be seen as a form of civil disobedience or online protest. In this view, DDoS attacks are akin to sit-ins or other forms of peaceful protest, used to draw attention to an issue or cause.

Ethical Hacking: Ethical hacking, also known as "white hat" hacking, involves using hacking skills to identify and fix vulnerabilities in systems. Ethical hackers can play a crucial role in preventing DDoS attacks by identifying potential weaknesses that could be exploited and helping organizations strengthen their defenses.

In conclusion, while DDoS attacks are generally considered illegal and unethical, there are complex legal and ethical issues surrounding their use. It's crucial for individuals and organizations to understand these aspects and navigate them carefully.

Future Trends and Predictions for DDoS Attacks

The Evolution of DDoS Attacks

The ever-evolving threat landscape of Distributed Denial-of-Service (DDoS) attacks poses a significant challenge to online businesses and critical infrastructure. This section delves into the anticipated future of DDoS attacks, examining emerging trends and potential developments based on the latest research and insights from industry reports like Radware's 2023 DDoS Report.

The Metamorphosis of DDoS Attacks

DDoS attacks are undergoing a metamorphosis, becoming increasingly sophisticated, diverse, and impactful. The 2023 Radware report highlights a concerning 44% increase in the average attack size compared to the previous year, showcasing the escalating threat. This transformation is driven by several key factors:

Expanding Attack Landscape: Attackers are actively exploring new avenues, including:

IoT Botnets: The vast and often poorly secured landscape of Internet-of-Things (IoT) devices presents a fertile ground for building powerful botnets capable of launching devastating attacks.

Application-Layer Attacks: These attacks target specific vulnerabilities in applications, bypassing traditional network-based defenses and potentially causing significant damage.

Multi-Vector Attacks: Combining multiple attack techniques, such as volumetric and application-layer attacks, overwhelms defenses and makes them more difficult to mitigate.

DaaS Proliferation: The rise of readily available DDoS-as-a-service (DaaS) offerings simplifies attack orchestration, making them accessible even to less-skilled actors. This democratization of DDoS attacks lowers the barrier to entry and broadens the potential pool of attackers.

Shifting Motivations: DDoS attacks are increasingly employed as a diversionary tactic for more nefarious activities like:

Data Breaches: By overwhelming a network with traffic, attackers can distract security personnel and create an opening to steal sensitive data.

Ransomware Attacks: DDoS attacks can be used to disrupt operations and pressure organizations into paying ransom demands.

Extortion Schemes: Threat actors may launch DDoS attacks against businesses or individuals and demand extortion payments to cease the attack. This convergence of attack methods with other cybercrimes creates a complex and multifaceted threat landscape.

The Rise of the Machines: Emerging Technologies in DDoS Defense

To combat these evolving threats, innovative defense technologies are also emerging:

Machine Learning (ML): ML algorithms offer real-time identification and mitigation of malicious traffic, adapting to novel attack patterns. For instance, Radware's DefensePro leverages ML-powered anomaly detection for proactive attack mitigation. By analyzing network traffic patterns and user behavior, ML can differentiate between legitimate users and malicious actors, enabling faster and more effective response.

Cloud-based Security: Cloud-based DDoS mitigation solutions provide several advantages:

Scalability: They can seamlessly handle large-scale attacks by leveraging the vast resources of the cloud provider, eliminating the need for significant on-premises infrastructure investment.

Global Reach: With geographically distributed points of presence, cloud-based solutions can effectively mitigate attacks originating from diverse locations.

Flexibility: Cloud-based solutions offer a subscription-based model, allowing organizations to scale their defenses up or down as needed, optimizing costs and resource allocation.

Behavioral Analytics: By analyzing user behavior patterns and establishing baselines, organizations can enhance their ability to distinguish legitimate traffic from malicious activity. This involves monitoring factors like log-in attempts, access times, and data usage patterns to identify deviations that might indicate suspicious activity. By combining behavioral analytics with other security measures, organizations can create a more comprehensive and layered defense against DDoS attacks.

Predicting the Future Landscape of DDoS Attacks

Several key trends are likely to shape the future of DDoS attacks:

Targeted Attacks on Critical Infrastructure: Critical infrastructure, such as power grids, financial institutions, and healthcare providers, may become more susceptible to targeted DDoS attacks aimed at causing widespread disruption and potentially jeopardizing public safety. The potential impact of such attacks necessitates robust defenses and coordinated response strategies among government agencies, critical infrastructure operators, and cybersecurity professionals.

AI-powered Attacks: Attackers may leverage artificial intelligence (AI) to automate and personalize attacks, making them more challenging to detect and mitigate. AI could be used to:

- Identify and exploit vulnerabilities in an organization's defenses.
- Launch coordinated attacks that adapt to ongoing mitigation efforts.
- Generate highly targeted phishing and social engineering attacks that are more likely to trick users.

Emergence of "Mega-Attacks": The growing number of connected devices, the widespread adoption of IPv6, and the increasing availability of powerful botnets could facilitate the launch of larger and more complex attacks with the potential to cripple critical infrastructure and online services.

Increased Geopolitical Implications: In a world rife with geopolitical tensions, DDoS attacks may be used as tools of cyberwarfare, aimed at disrupting rival nations' infrastructure, or influencing public opinion. Proactive measures and international collaboration will be crucial to mitigate the impact of such attacks.

Related Articles

What Is a Web DDoS Tsunami Attack?
Web DDoS Tsunami attacks combine application layer attack vectors, leveraging new tools to create sophisticated attacks that are harder—and sometimes impossible—to detect and mitigate with traditional methods.

What Is the Difference Between DoS and DDoS Attacks?
In a distributed denial-of-service (DDoS) attack, hackers flood a target website with so much traffic from multiple systems that it is rendered inaccessible to legitimate users.

How to DDoS? Seven Common DDoS Attack Tools
Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are malicious attempts to disrupt online services by flooding them with massive amounts of traffic from multiple sources.

Scrubbing Center
A centralized data cleansing station where traffic is analyzed and malicious traffic (ddos, known vulnerabilities and exploits) is removed.

Application Security In A Multi-Cloud World 2023

The "great cloud migration" is looking different than how it was originally touted, with few organizations hosting all their applications exclusively on public cloud platforms.

Read more ⟶

Choosing The Right DDoS Solution

A guide to DDoS solutions and how to select the optimal solution for your organization

Read more ⟶

Layer 7 DDoS Attacks To Prepare For & Mitigation Capabilities To Stop Them

This guide outlines the top DDoS attack vectors now targeting applications and mitigation capabilities you should consider to mitigate the threats

Read more ⟶

2024 Global Threat Analysis Report

Understand the statistics, trends and hacktivist activity that made an impact throughout 2023.

Read more ⟶

Contact Radware Sales

Our experts will answer your questions, assess your needs, and help you understand which products are best for your business.

CONTACT US NOW

Already a Customer?

We're ready to help, whether you need support, additional services, or answers to your questions about our products and solutions.

- Locations
- Get Answers Now from KnowledgeBase
- Get Free Online Product Training
- Engage with Radware Technical Support
- Join the Radware Customer Program

Get Social

Connect with experts and join the conversation about Radware technologies.

- Blog
- Security Research Center
- CyberPedia

ABOUT RADWARE
Customers
Partners
Investor Relations
Diversity & Inclusion
Corporate Responsibility
Careers
Locations
Contact Us

ONLINE SERVICES
Support
Training
Portals
Cloud Services Portal
Support Forum
Knowledge Base
Professional Services

NEWS ROOM
Press Releases
Media Coverage
Digital Events
In Person Events
Awards
Certifications

ENGAGE WITH US
Blog
Live Threat Map

© Copyright 2024 Radware – All Rights Reserved.